Cassandra Crossing/ Sensori spioni a profusione

(417)—Pedometri, cardiofrequenzimetri, microfoni, GPS… ma quanti ce ne sono negli oggetti che usiamo e indossiamo ogni giorno? Laddove…

Cassandra Crossing/ Sensori spioni a profusione
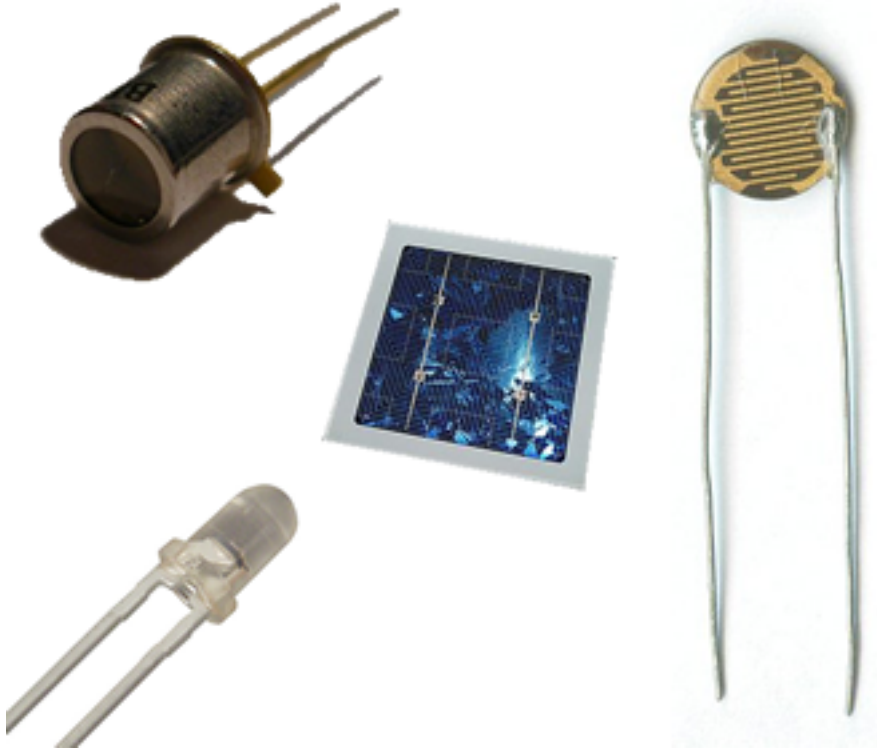
Figure 1: https://en.wikipedia.org/wiki/Sensor#/media/File:Light_sensor.png

(417)—Pedometri, cardiofrequenzimetri, microfoni, GPS… ma quanti ce ne sono negli oggetti che usiamo e indossiamo ogni giorno? Laddove non sia possibile farne a meno, però, è meglio limitare i danni.

18 ottobre 2017—Già anni or sono, per la precisione nel 2006, Cassandra metteva in allarme i suoi 24 innocenti lettori dalla possibilità di essere abusati e di subire "prelievi" malandrini di dati personali.
Si trattava della questione dei "canali di ritorno" per via telefonica, che i sintonizzatori per le pay TV e in generale le set-top box iniziavano ad avere ben 11 anni fa.

Parecchi anni dopo, per l'esattezza nel 2012, Cassandra stressava nuovamente i 24 imperturbabili lettori, mettendo in evidenza come la loro smart-TV in salotto li stesse spiando.

Malgrado gli allarmi dati con largo anticipo (non siam profeti mica per niente!) non è che i 24 inossidabili lettori si fossero agitati più di tanto.

Bene, per quanto riguarda i sensori e i dati, spesso biometrici, che essi captano e forniscono, di allarmi ce ne sono stati a bizzeffe, tanto che non serve inserire ulteriori link ad articoli, sia cassandreschi che non.

Vale però la pena dedicare una serissima nota, anche se breve, alla **crescente quantità di sensori che ci sta circondando**, nascosti nei nuovi oggetti di uso comune e meno comune che acquistiamo.

Non è infatti concepibile che a fronte di un aggravamento dei problemi di privacy creato dagli oggetti che catturano dati da noi generati, entrando nelle nostre case o attaccandosi ai nostri corpi, corrisponda un calo, anzi un **annullamento dell'attenzione al problema**.

Ogni sensore intorno a noi o su di noi estrae uno specifico tipo di dati e lo invia ad una destinazione.

E' banale capire che il danno che ne deriva è grossomodo proporzionale al numero di sensori che ci intercettano."Numero di sensori"? Sì, sensori ce ne sono ormai a bizzeffe.

Mentre un telefono non smart ne contiene solo due, un sensore di rilevamento di posizione (i dati di cella GSM) ed un microfono, **uno smartphone moderno ne contiene probabilmente** da 9 a 12 tra cui: microfono, telecamera anteriore, telecamera posteriore, posizione GSM, posizione GPS, accelerometro bussola, sensore di illuminazione, sensore di prossimità, giroscopio, sensore per lettura contactless, lettore di impronte digitale.

E se pensate che telecamere e microfono non siano sensori perché funzionano solo quando volete voi… non sapete quanto Galileo, FinFisher e loro simili siano di uso comune… ma questa è un'altra storia.

Torniamo al nostro conteggio di sensori; **una "scatola nera" associata alla polizza di assicurazione auto ne contiene 6**: microfono, posizione GPS, posizione GSM, accelerometro, sensore di velocità, parametri auto (posizione Gas, Freno, Frizione, Cambio); **un braccialetto fitness 3 o 4**: pedometro (contapassi), cardiofrequenzimetro a LED, barometro, posizione GPS (alcuni modelli); **un laptop almeno 2**: microfono e telecamera. In generale, **3 su 4 oggetti possiedono un microfono**.

La cosa vi lascia davvero tranquilli perché tanto non avete nulla da nascondere?

I canali di ritorno, di cui parlava il precedente articolo del 2006, non sono più l'eccezione ma la regola; sono tipicamente la rete WiFi e/o la rete GSM 3G/4G, ormai così comuni da aver praticamente soppiantato le vecchie linee telefoniche non solo come canale di ritorno, ma anche nell'uso comune.

L'importanza, o meglio **la pericolosità dei dati raccolti da un sensore varia molto a seconda del tipo e della quantità di dati rilevati**.

In generale i dati biometrici sono i più critici; il solo cardiofrequenzimetro rileva non solo il tipo di attività che state svolgendo (sì, pure "quello") ma anche altre informazioni importanti sul vostro stato di salute.Ai sensori propriamente detti si aggiungono le app e i programmi che "telefonano a casa" (cioè praticamente tutti); sono "sensori" che, pur non intercettando direttamente dati, ne moltiplicano la diffusione.

Esempi comunissimi di **dati vendemmiati a profusione dalle app sono i dati di geolocalizzazione e l'accesso alla rubrica**.

Visto che viviamo in una società in cui la privacy è diventata un esercizio per pochi paranoici, perché non applicare almeno **semplici strategie di limitazione del danno**.

La geolocalizzazione ad esempio: basta attivarla solo quando serve e disattivarla subito dopo. Le autorizzazioni delle app: dopo aver installato una nuova app e prima di lanciarla, visitate la pagina dei settaggi che vi consente di disattivarle. E già che ci siete, controllate le autorizzazioni delle applicazioni già installate, togliendo tutte quelle che non sembrano indispensabili; tanto se

l'app smettesse di funzionare potete sempre decidere di rimetterle (ma molto meglio cancellare l'app malandrina). E poi, quante app potete cancellare perché tanto non le usate mai?La limitazione del danno è la nuova frontiera dei paranoici.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on April 13, 2021.

Canonical link

Exported from Medium on August 27, 2025.